Enterprise Security Tactical Plan

Fiscal Years 2011 – 2012

(July 1, 2010 to June 30, 2012)

Prepared By:

State Chief Information Security Officer

The Information Security Council

658 Cedar Street Saint Paul, MN 55155 www.oet.state.mn.us

State of Minnesota
Enterprise Security Tactical Plan

Contents

Executive Summary

The Information Security Council (ISC) and State Chief Information Security Officer are pleased to present the updated Enterprise Security Tactical Plan for the State of Minnesota. This two-year plan prioritizes the tactical initiatives for the management, control, and protection of information assets. It also will help achieve the three strategic principles in the Enterprise Security Strategic Plan:

- **Improved situational awareness**, which includes continuous system monitoring and assessment of controls;
- **Proactive risk management**, such as solidly articulated requirements and ongoing security training; and
- **Robust crisis and security incident management**, which allows critical services to continue uninterrupted in a crisis.

The priorities and scope of the tactical initiatives in this plan could change over time. For example, due to reductions in Enterprise Security Program funding, the ISC has scaled back the scope of a Security Incident and Event Management initiative, started in fiscal year 2009. Conversely, the scopes of other security initiatives have been expanded in response to the planned statewide data center co-location and other Minnesota iGov planning efforts.

It is important to note that this plan does not cover the full breadth of security work being done by state agencies or the Information Security Council. Though not depicted in this plan, many operational activities happen each day that are vital to the security of the State's information.

Introduction

With help from the Information Security Council, the Chief Information Security Officer worked to create the following **mission** for the Enterprise Security Program:

> *"The Enterprise Security Program exists to support the efficient delivery of services to government entities and their customers; through a sustainable information security program.*
>
> *The program will accomplish its mission through enterprise information security policies, standards, guidelines, and services that protect the state's information assets and the security interests of the users of state services."*

This plan outlines the tactical initiatives the State of Minnesota is undertaking over the next two years. These initiatives align with the following ten priorities identified in the Enterprise Security Strategic Plan:

- All state computer systems are continuously monitored for adverse information security events
- Government leaders at the highest levels understand and support the information security program
- All state employees receive ongoing security training appropriate to their job duties
- Information security program requirements are clearly articulated in a framework of policies, procedures, and standards
- Exploitable technical vulnerabilities in state computer systems are promptly identified and remediated
- People and entities that conduct business with state government have appropriate and timely access to the necessary computer resources and data
- State computer resources and data are protected from being used or accessed inappropriately
- The Office of Enterprise Technology serves as a leader by setting high standards for excellence in information security
- When information security incidents occur, government entities promptly contain, remediate, and manage those incidents
- Mission-critical services will continue in the event of a crisis

Key Initiatives

The Enterprise Security Tactical Plan refers to high priority security activities as "**key initiatives.**" In some cases, active projects are already underway for key initiatives, while others are in the planning stage.

It is important to understand that this plan is not a complete inventory of work being done by the Information Security Council or state agency security professionals. Many day-to-day operational duties, such as assisting with the secure development of new government computer systems, are not in this plan.

Each key initiative has a narrative that describes why it is a high priority and the anticipated security benefits. This plan also outlines milestones for each key initiative, with anticipated dates for the achievement of those milestones. Finally, as illustrated in Figure 1, the plan includes a graphical depiction of how each key initiative links to outcomes the Enterprise Security Strategic Plan.

Figure 1
Linking Key Initiatives to Strategic Priorities

Description: A brief description of the tactical initiative.

Key Benefits:
- A list of the key benefits that will be achieved through this effort

Key Milestones

Milestone Descriptions	Projected Due Date
Milestone #1	
Milestone #2	
Milestone #3	

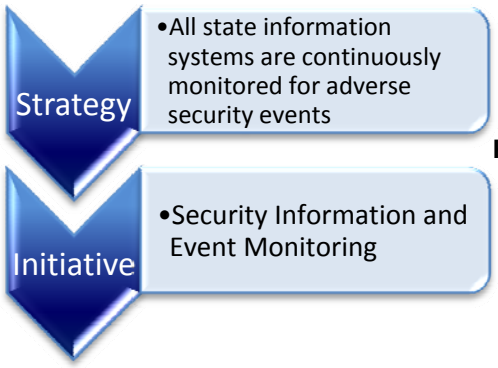
Chapter 1: Improved Situational Awareness

Initiatives in this category will help the state obtain a better understanding of its risk posture and promptly respond to adverse events. They also will give the State the ability to measure its risk posture with rigorous performance metrics.

Initiative #1 – Security Information and Event Management

Security information and event management (SIEM) is a solution for aggregating, correlating, and analyzing security event data in real time. SIEM solutions help organizations identify and promptly respond to threats, demonstrate compliance with regulatory requirements, and perform sophisticated forensic activities.

This initiative will further expand the extensive implementation of SIEM technology that is now in Office of Enterprise Technology (OET) data centers. It moves the previous SIEM pilot initiative forward to an enterprise-wide deployment strategy. As data center co-location and consolidation progresses, this SIEM technology roadmap will provide robust monitoring capabilities to all data centers managed by the Office of Enterprise Technology as a utility service.



Description: Define core requirements for enterprise-wide security monitoring, and implementation of these practices within OET.

Key Benefits:

- Improved ability to identify complex cyber attacks
- Reduced time and cost to investigate security incidents
- Consistent and robust monitoring of all agencies, including those with limited resources

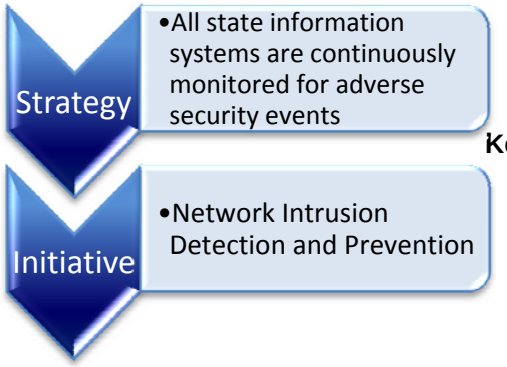
Key Milestones

Milestone Descriptions	Projected Due Date
Customer implementation incorporated into monitoring solution designed	11/2010
SIEM infrastructure for new data centers design	12/2010
Enterprise-wide SIEM business plan developed	03/2011
SIEM operational manual with documented processes completed	06/2011
SIEM service-related documentation developed	06/2011
Enterprise procedures for information and event management published	06/2011
SIEM service offering funded, available, and integrated	06/2011
Existing SIEM solutions centralized	06/2011
SIEM training materials and schedule developed	12/2011
Required SIEM components for monitoring, logging and correlating of priority one and two applications purchased	06/2012
OET event monitoring, logging and correlation based on risk posture and compliance requirements implemented	06/2012

Initiative #2 – Network Intrusion Detection and Prevention

Network intrusion detection and prevention (IDP) monitors and analyzes network traffic for potentially malicious security events. Through the network IDP solution, security professionals can identify and promptly respond to threats, demonstrate compliance with regulatory requirements, and perform complex forensics. In very mature environments, network IDP can be used to block malicious network traffic before it can cause harm. This service is an important source of information for a robust SIEM solution; hence it is called out as a separate initiative.

The network intrusion detection and prevention solution is an enterprise-wide utility service. The implementation plan is dependent on funding availability. However, data center co-location will provide a unique opportunity to deliver this service to all agencies in a cost efficient manner. This initiative includes continuous improvement of the support processes developed for the agencies that are now utilizing this Office of Enterprise Technology service.



Description: Define core requirements for enterprise-wide security monitoring, and implementation of these practices within OET.

Key Benefits:

- Improved capability to discern complex cyber attacks and attack trending
- Real time alerting of potential security incidents with automated attack response capability
- Consistent and robust security monitoring capabilities across the network

Key Milestones

Milestone Descriptions	Projected Due Date
Funding model for 7/24/365 coverage designed	11/2010
IDP solution for enterprise data centers designed	11/2010
Funding model for IDP service designed	12/2010
Roadmap for IDP implementation across agencies and counties designed	03/2011
IDP solution for new enterprise data center purchased and implemented	03/2011
Existing IDP solution centralized	06/2011
Coarse tuning IDP monitoring priority one and two systems completed	09/2011
Performance and efficiency metrics measurement selected	09/2011
Performance and efficiency metric baselines defined	12/2011
IDP sensors in all four state data centers implemented	06/2012
Metric data gathered, processed, analyzed and presentation method designed	06/2012

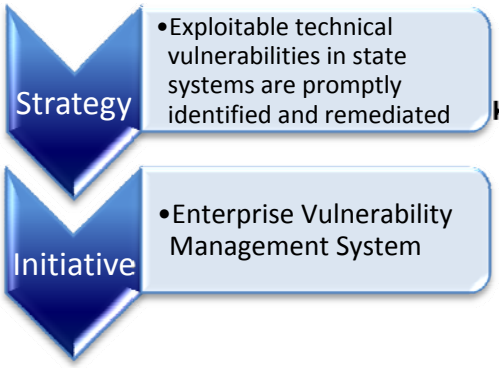
Chapter 2: Proactive Risk Management

Initiatives in this category will make employees and government leaders more aware of security threats. They also will help garner the executive support needed for the Enterprise Security Program to thrive long-term. Finally, initiatives in this category include the implementation of preventive security controls, such as proactive vulnerability management.

Initiative #3 – Enterprise Vulnerability and Threat Management

This key initiative provides a proactive approach to identify and mitigate security vulnerabilities before they can be exploited by hackers. Technologies in place today allow for the continuous assessment of the State's information systems. These tools are augmented by the ongoing dissemination of threat and vulnerability information to all state agencies.

All executive branch agencies are utilizing the Enterprise Vulnerability Management System. This initiative is continuously improving the identified processes, including more standardized reporting and an expanded threat dissemination service. EVMS is an enterprise-wide utility service, and will continue to be so in the future.



Description: Central system to provide ongoing vulnerability assessments of all information technology assets.

Key Benefits:

- State finds and remediates problems before they are exploited by hackers
- Inventory of all technology assets ranked by priority
- Services offered to all agencies, including those with limited resources

Key Milestones

Milestone Descriptions	Projected Due Date
Threat Advisory process fully operational across Executive Branch	12/2010
Standardized scanning across Executive Branch implemented	06/2011
SIH deployed across Executive Branch	06/2011
Performance and efficiency metrics measurement selected	09/2011
SIH custom reports developed	12/2011
Performance and efficiency metric baselines defined	12/2011
Metric data gathered, processed, analyzed and presentation method designed	06/2012
Additional tools for the EVMS service designed and integrated	06/2012
Enterprise application assessment process for select critical applications established	06/2012

Initiative #4 – Enterprise Security Program Framework

This key initiative establishes a policy-based foundation for the Enterprise Security Program. The Information Security Council made a decision to build the security program using a framework developed by the National Institute of Standards and Technology (NIST).

Over the past two years, the security community has worked to define, vet, and adopt a series of baseline security policies and standards consistent with the NIST framework. These policies and standards flow through a collaborative governance process that includes agency Chief Information Officers and the State Chief Information Officer.

During the two years this plan covers, this initiative will result in the completion of the remaining baseline security policies and standards. Also, this initiative will yield a series of key performance metrics to measure and report on the State's risk posture.

Description: Complete enterprise security policy and standard framework with a program governance model for continuous improvement.

Key Benefits:

- Clear security baselines for all government entities
- Policy-based foundation to measure results
- Consistent application of security controls across the enterprise

Key Milestones

Milestone Description	Projected Due Date
Initial standards to support policies published	03/2011
Standardized performance reporting improvement of program established	06/2011
Process for continuous improvement of program published	06/2011
Annual program performance reporting established	07/2011
Program compliance and audit plan established	07/2011
Security architecture is integrated into the Enterprise Architecture	12/2011
Third-party security requirements established	12/2011
First enterprise wide compliance assessment report published	06/2012
Enterprise security standards' requirements established across Executive branch	06/2012
Enterprise security services integrated into co-located data centers	06/2012

Initiative #5 – Information Risk Management Program

This initiative will define an enterprise risk management framework that will be used to identify security risks to the State's information assets. This includes foundational processes to ensure that security controls are architected into new information systems from the onset. It also will ensure that residual risks are understood and accepted by management before systems are moved into production. Recognizing that risks change over time, a key outcome of this effort will be a process to continuously reassess security controls as information systems mature. Finally, to be useful, the Risk Management Program must provide ongoing and meaningful metrics to executives for informed decision making.

Description: Enterprise-wide risk management processes to enable better risk-based decisions by government entities' leaders.

Key Benefits:

- Better understanding of the enterprise risk profile
- Better understanding by government entities of their information security risks
- Consistent delivery of security controls through security plans and security authorization

Key Milestones:

Milestone Descriptions	Projected Due Date
Enterprise Security Risk Management standards published	12/2010
Enterprise Security Risk Management processes and guidelines published	03/2011
Data center co-location security risk assessment completed	06/2011
Enterprise Security Risk Management requirements and processes integrated into managed services	06/2011
Enterprise Security Risk Management processes utilized across Executive Branch for critical information assets	12/2011
Initial Enterprise Security Risk Gap Report published	03/2012
First Enterprise-wide risk posture report delivered to Governor's office	06/2012
Third-Party Risk Management & Compliance	
Third-party risk assessment processes defined	03/2011
Third-party monitoring requirements defined	03/2011
Third-party compliance deliverables defined	06/2011
Third-party compliance methodology established	06/2012

Initiative #6 – Security Planning & Life Cycle for Application Development

Agencies that contract for software development or have application development teams need to incorporate secure coding practices and security requirements into the software development process. Ongoing management of applications and secure development practices also must be tightly coupled with requirements in the State's Enterprise Architecture (EA) program. As the State's EA program matures, so will the disciplines surrounding application development and secure coding.

This initiative is currently limited due to resource constraints. However, the Enterprise Security Office and security community recognize that it is important to start with a solid policy and process foundation. Therefore, as part of the broader information risk management practices, this initiative is being launched to begin addressing secure software development requirements. This initiative has also impacted the Training & Awareness initiative (#7) by identifying the need to train developers in secure coding practices and the Vulnerability Management initiative (#3) by requiring the establishment of an application vulnerability assessment process.

Description: Enterprise-wide risk management processes to enable better risk-based decisions by government entities' leaders.

Key Benefits:

- Reduced costs for addressing design-level security vulnerabilities
- Constant approach for identifying and addressing security risk in all software used by the State

Key Milestones:

Milestone Descriptions	Projected Due Date
Secure Development Collaboration Team established	12/2010
Enterprise Security Planning & Life Cycle standards published	03/2011
Enterprise Security Planning & Life Cycle processes and guidelines published	06/2011
Enterprise Security Development Methodology Frameworks defined	06/2012
Third-Party Risk Management & Compliance	
Third-party software development control requirements defined	06/2011
Third-party contract language for secure software (custom developed or off the shelf software) defined	06/2011

Initiative #7 – Security Awareness for Employees & Government Leaders

Employees are often the weakest link in an organization's security defenses. Therefore, it is important to educate employees so that they understand pertinent security risks and know what needs to be done to protect resources and data.

Current resource restraints will continue to impede our ability to achieve all of our security awareness strategic goals. However, this initiative will make sure that the State of Minnesota makes some progress during this biennium. Milestones identified below will provide a minimal level of security awareness and create a baseline set of requirements for the future. It is important to stress that the Information Security Council will continue to host critical security training to the extent that resources permit.

Description: Ongoing and comprehensive security awareness program for all state employees and government leaders / policymakers.

Key Benefits:

- Better awareness of security threats capable of impacting government operations
- Fewer security incidents caused by employee mistakes
- Common baseline of knowledge for all employees
- Clear understanding of all enterprise security initiatives
- Support for the Enterprise Security Program

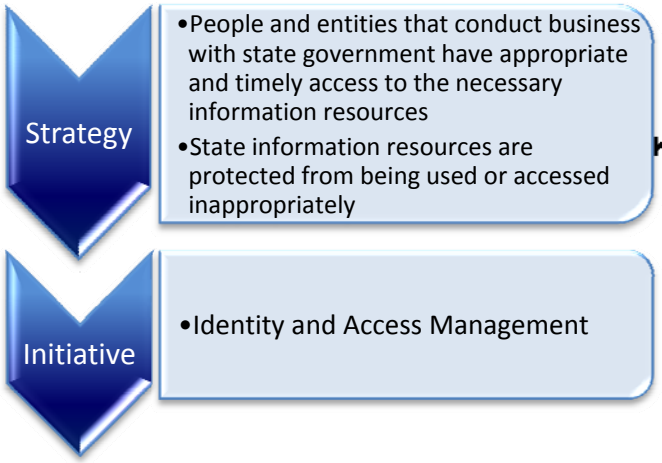
Key Milestones

Milestone Descriptions	Projected Due Date
Annual State Cyber-Security Awareness Month campaign held	10/2010 & 10/2011
Enterprise Security Awareness & Training Standard published	12/2010
Annual Secure Software Development Training session held	06/2011 & 06/2012
Annual Government Leaders Security Retreat held	01/2011
Enterprise Security Awareness Program plan developed	06/2011
Enterprise Security Awareness process developed	12/2011
Enterprise Security Awareness materials developed	06/2012

Initiative #8 – Identity and Access Management

To ensure the efficient ongoing delivery of government services the State must identify core business processes that are shared across agencies and in many cases across branches of government. Related standards and methods of automation must then be developed and implemented to execute these business processes with minimal operational overhead. Identity and access management concepts represent a foundational element of this business model.

The State's Identity and Access Management (IAM) program exists to define core business processes related to management of user identities and access to government systems and data. The program exists to establish consensus among stakeholders on related standards. Finally, the program exists to define and implement a common set of technology tools for automation of IAM related business processes.



Description: Centralized and streamlined access control solution for state government.

Key Benefits:

- Better security through uniform and repeatable access control processes
- Better experience for users of state services by providing all access through a single user ID and password
- Reduced costs to develop new government systems by leveraging an external access control solution

Key Milestones

Milestone Descriptions	Projected Due Date
Requirements for initial rollout of a shared Identity and Access Management solution identified	12/2010
Technical solution to address business functions designed	02/2011
Implementation plan for the technical solution created	03/2011
Migration plan for customers of existing IAM functionality created	04/2011
IAM technical solution to address business functions implemented	06/2011
Migration of existing IAM customers to new IAM technical solution completed	09/2011
Existing IAM technical implementations retired	12/2011
Expand new IAM technical solution functionality to address business requirements for other state agencies	06/2012

Initiative #9 – Office of Enterprise Technology Security Program

This initiative, started in fiscal year 2008, will enhance and mature Office of Enterprise Technology's (OET) security to be a best-in-class information security program. OET must be a security center of excellence because it houses many critical government computer systems and sensitive data. The proposed data center co-location effort will compound the need for extremely robust preventative, detective, and corrective security controls in the central technology agency.

Under this initiative, OET will serve as a leader by piloting new security technologies and developing robust processes that can be leveraged by all agencies. OET will also lead statewide efforts to define secure configuration standards for software and hardware products.

Description: Develop and institute a robust information security program to protect the confidentiality, availability, and integrity of data and information systems assets managed by OET.

Key Benefits:

- Able to comply with the Enterprise Security Program and applicable business and regulatory requirements
- Long term diligence in protecting data and systems entrusted to OET's care
- OET Information Security Program can serve as an example for agency security programs

Key Milestones

Milestone Descriptions	Projected Due Date
OET Core Program Security Standards published	01/2011
OET ongoing Security Program training requirements are defined	03/2011
OET Security Program requirements for OET project management processes defined and integrated	06/2011
Process for defining, measuring, and reviewing OET security performance metrics implemented	06/2011
Defined and repeatable remediation processes and procedures for OET Vulnerability Management implemented	08/2011
Risk mitigation processes and procedures developed and implemented	01/2012
Situational awareness processes to remediate root cause operational process and architectural design flaw risks implemented	06/2012

Chapter 3: Robust Crisis and Security Incident Management

Initiatives in this category will help the State of Minnesota promptly respond to and manage security incidents to minimize damage. They also will help the State continue mission critical services in times of crisis.

Initiative #10 – Enterprise Business Continuity Program

History has shown that even well managed services can become victims of catastrophic failure. The Enterprise Business Continuity Program helps mitigate these risks through detailed planning activities, including business impact analysis, recovery strategy development, business continuity planning, and disaster recovery exercises.

This ongoing initiative will facilitate the prioritization of services for the State as a whole and define appropriate recovery strategies for critical information systems. It also will help move the State closer to compliance with the enterprise policy and standard for continuity of operations.

Description: Ongoing continuity program to address unanticipated disruptions to government services

Key Benefits:

- Faster recovery of priority government services during a crisis
- Reduced costs through leveraging shared recovery environment
- Better ability to share staff during times of crisis through adoption of a common plan format, processes, and tools

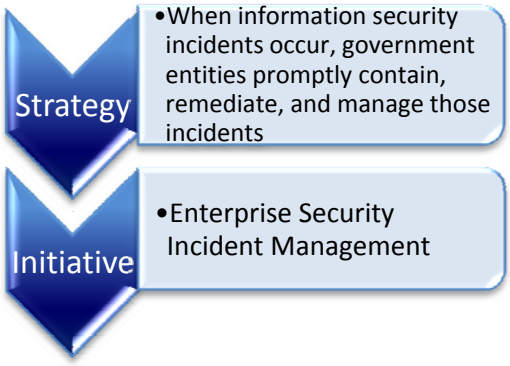
Key Milestones

Milestone Descriptions	Projected Due Date
Enterprise Continuity of Operations Program progress monitoring for all agencies initiated	11/2010
Enterprise technology recovery strategies developed	06/2011
Enterprise training for all agency business continuity planners completed	09/2011
OET Continuity of Operations plans and technology recovery strategies developed	10/2011
Enterprise Living Disaster Recovery Planning System (LDRPS) functionality and efficiency enhancements completed	12/2011
OET Continuity of Operations recovery strategies implemented	06/2012

Initiative #11 – Enterprise Security Incident Management

Security incident management and computer forensics seek to determine the cause, scope, and impact of incidents. The goal of incident management is to stop unwanted activity, limit damage, and prevent recurrence.

The Enterprise Security Office and Information Security Council have worked to develop incident response and data forensic processes. This initiative will now work to install these processes in all executive branch agencies as a shared utility service. Adopting a collaborative approach will improve the State's ability to identify and isolate incidents, thereby limiting damage.



Description: Enterprise-wide approach to record, identify, and manage information security incidents.

Key Benefits:

- Ability to limit damage through information sharing
- Fewer cross-agency infections
- Reduced costs through the sharing of staff and expensive forensic investigation tools

Key Milestones:

Milestone Descriptions	Projected Due Date
Security incident management training materials developed	12/2010
Data practices procedure for security incident data requests developed	12/2010
Metric reporting tool selected and implemented	06/2011
Whitepaper on malware behavioral analysis tools developed	06/2011
Whitepaper on enterprise forensic and e-discovery tools developed	09/2011
Homeland Security Grant request for needed tools submitted	02/2012
Participated in authorized national cyber incident exercises	06/2012
Non law enforcement data forensic labs integrated	06/2012
Performance and efficiency metrics measurement selected	06/2012
Performance and efficiency metric baselines defined	06/2012
Metric data gathered, processed, analyzed and presentation method designed	06/2012